CLAIMS

1. An information sending system for sending data using a data sending device and a data receiving device, characterized in that

said data sending device comprises:

sending end controlling means for encrypting said data with predetermined key data, generating handling policy data describing handling policy of said data, and generating a signature for said encrypted data and said handling policy data; and

sending means for sending the signature for said encrypted data and said handling policy data to said data receiving device together with said encrypted data and said handling policy data, and

said data receiving device comprises:

receiving means for receiving the signature for said encrypted data and said handling policy data together with said encrypted data and said handling policy data; and

receiving end controlling means for verifying said received signature, and comparing creator identification data included in said data with creator identification data included in said handling policy data.

2. An information sending system for sending data using a data sending device and a data receiving device, characterized in that

said data sending device comprises:

sending end controlling means for encrypting said data with predetermined key data, generating handling policy data describing

handling policy of said data, and generating signatures separately for said encrypted data and said handling policy data; and

sending means for sending said signatures for data and for handling policy to said data receiving device together with said encrypted data and said handling policy data, and

said data receiving device comprises:

receiving means for receiving said signatures for data and for handling policy together with said encrypted data and said handling policy data; and

receiving end comparing means for verifying said signature for data and said signature for handling policy, and comparing creator identification data included in said data with creator identification data included in said handling policy data.

3. An information sending system for sending data using a data sending device and a data receiving device, characterized in that

said data sending device comprises:

sending end controlling means for encrypting said data with predetermined key data, generating handling policy data describing handling policy of said data, and generating a signature for a secure container for said encrypted data and said handling policy data; and

sending means for sending the signature for the secure container for said encrypted data and said handling policy data to said data receiving device together with said encrypted data and said handling policy data, and

said data receiving device comprises:

receiving means for receiving the signature for the secure container for said encrypted data and said handling policy data together with said encrypted data and said handling policy data; and

receiving end controlling means for verifying said signature for the secure container.

4. An information sending system for sending data using a data sending device and a data receiving device, characterized in that

said data sending device comprises:

sending end controlling means for encrypting said data with predetermined key data, generating handling policy data describing handling policy of said data, generating a signature for data for said encrypted data, and generating a signature for handling policy for said handling policy data and said signature for data; and

sending means for sending said encrypted data, said signature for data, said handling policy data and said signature for handling policy to said data receiving device, and

said data receiving device comprises:

receiving means for receiving said encrypted data, said signature for data, said handling policy data and said signature for handling policy; and

receiving end controlling means for verifying said signature for data and said signature for handling policy.

5. An information sending system for sending data using a data sending device and a data receiving device, characterized in that

said data sending device comprises:

sending end controlling means for encrypting said data with predetermined key data, generating handling policy data describing handling policy of said data, generating a signature for handling policy data for said handling policy data, and generating a signature for data for said encrypted data and said signature for handling policy; and

sending means for sending said encrypted data, said signature for data, said handling policy data and said signature for handling policy to said data receiving device, and

said data receiving device comprises:

receiving means for receiving said encrypted data, said signature for data, said handling policy data and said signature for handling policy; and

verifying means for verifying said signature for data and said signature for handling policy.

6. The information sending system according to Claim 1,

characterized in that

said sending end controlling means stores encrypted key data with key data for encrypting said data encrypted with a distribution key, and generates a signature for key data for said encrypted key data,

said sending means sends said generated signature for key data to said data receiving device,

said receiving means receives said key data, and

said receiving end controlling means verifies said signature for key data.

7. The information sending system according to Claim 3, characterized in that

said sending end controlling means stores encrypted key data with key data for encrypting said data encrypted with a distribution key, and generates a signature for secure containers for said encrypted data, said encrypted key data and said handling policy,

said sending means sends said encrypted data, said encrypted key data, said handling policy data and said signature for secure containers to said data receiving device,

said receiving means receives said encrypted data, said encrypted key data, said handling policy data and said signature for secure containers, and

said receiving end controlling means verifies said signature for secure containers.

8. An information sending method for sending data using a data sending device and a data receiving device, characterized by comprising:

a sending step of encrypting said data with predetermined key data, generating handling policy data describing handling policy of said data, generating a signature for said encrypted data and said handling policy data, and sending the same to said data receiving device together with said encrypted data and said handling policy data, by said data sending device; and

a comparing step of receiving the signature for said encrypted data and said handling policy data together with said encrypted data

and said handling policy data, verifying said signature, and comparing creator identification data included said data with creator identification data included in said handling policy data, by said data receiving device.

9. An information sending method for sending data using a data sending device and a data receiving device, characterized by comprising:

a sending step of encrypting said data with predetermined key data, generating handling policy data describing handling policy of said data, generating signatures separately for said encrypted data and said handling policy data, and sending the generated signature for data and the generated signature for handling policy to said data receiving device together with said encrypted data and said handling policy data, by said data sending device; and

a comparing step of receiving said signature for data and said signature for handling policy together with said encrypted data and said handling policy data, verifying said signature for data and said signature for handling policy, and comparing creator identification data included in said data with creator identification data included in said handling policy data, by said data receiving device.

10. An information sending method for sending data using a data sending device and a data receiving device, characterized by comprising:

a sending step of encrypting said data with predetermined key data, generating handling policy data describing handling policy of said data,

generating a signature for secure containers for said encrypted data and said handling policy data, and sending the same to said data receiving device together with said encrypted data and said handling policy data, by said data sending device; and

a verifying step of receiving the signature for secure containers for said encrypted data and said handling policy data together with said encrypted data and said handling policy data, and verifying said signature for secure containers, by said data receiving device.

11. An information sending method for sending data using a data sending device and a data receiving device, characterized by comprising:

a sending step of encrypting said data with predetermined key data, generating handling policy data describing handling policy of said data, generating a signature for data for said encrypted data, generating a signature for handling policy for said handling policy data and said signature for data, and sending said encrypted data, said signature for data, said handling policy data and said signature for handling policy to said data receiving device, by said data sending device; and

a verifying step of receiving said encrypted data, said signature for data, said handling policy data and said signature for handling policy, and verifying said signature for data and said signature for handling policy, by said data receiving device.

12. An information sending method for sending data using a data sending device and a data receiving device, characterized by comprising:

a sending step of encrypting said data with predetermined key data, generating handling policy data describing handling policy of said data, generating a signature for handling policy for said handling policy data, generating a signature for data for said encrypted data and said signature for handling policy, and sending said encrypted data, said signature for data, said handling policy data and said signature for handling policy to said data receiving device, by said data sending device; and

a verifying step of receiving said encrypted data, said signature for data, said handling policy data and said signature for handling policy, and verifying said signature for data and said signature for handling policy, by said data receiving device.

13. The information sending method according to Claim 8, characterized in that

in said sending step, encrypted key data with key data for encrypting said data with a distribution key is stored, a signature for key data for said encrypted key data is generated, and the generated signature for key data is sent to said data receiving device, and

in said verifying step, said signature for key data is verified.

14. The information sending method according to Claim 10, characterized in that

in said sending step, encrypted key data with key data for encrypting said data encrypted with a distribution key is stored, a signature for secure containers for said encrypted data, said encrypted key data and said handling policy is generated, and said encrypted data,

said encrypted key data, said handling policy data and said signature for secure containers are sent to said data receiving device, and

in said verifying step, said signature for secure containers is verified.

15. An information sending device for sending predetermined data to a data receiving device, characterized by comprising:

sending end controlling means for encrypting said data with predetermined key data, generating handling policy data describing handling policy of said data, and generating a signature for send of said encrypted data and said handling policy data; and

sending means for sending said signature to said data receiving device together with said encrypted data and said handling policy data.

16. The information sending device according to Claim 15, characterized in that said sending end controlling means encrypts said data including creator identification data with said key data, and generates said handling policy data including said creator identification data.

17. The information sending device according to Claim 15, characterized in that said sending end controlling means generates a signature for said encrypted data and said handling policy data.

18. The information sending device according to Claim 15, characterized in that said sending end controlling means generates signatures separately for said encrypted data and said handling policy data.

19. The information sending device according to Claim 15, characterized in that said sending end controlling means generates a signature for secure containers for said encrypted data and said handling policy data.

20. The information sending device according to Claim 15, characterized in that said sending end controlling means generates a signature for data for said encrypted data, and generates a signature for handling policy for said handling policy data and said signature for data.

21. The information sending device according to Claim 15, characterized in that said sending end controlling means generates a signature for handling policy for said handling policy data, and generates a signature for data for said encrypted data and said signature for handling policy.

22. The information sending device according to Claim 15, characterized in that

said sending end controlling means stores encrypted key data with key data for encrypting said data encrypted with a distribution key, and generates a signature for key data for said encrypted key data, and

said sending means sends said generated signature for key data to said data receiving device.

23. The information sending device according to Claim 19, characterized in that

said sending end controlling means stores encrypted key data with key data for encrypting said data encrypted with a distribution key, and generates a signature for secure containers for said encrypted data, said encrypted key data and said handling policy, and

said sending means sends said encrypted data, said encrypted key data, said handling policy data and said signature for secure containers to said data receiving device.

24. An information receiving device for receiving predetermined data sent from a data sending device, characterized by comprising:

receiving means for receiving said data encrypted with predetermined key data, handling policy data describing handling policy of the data, and a signature for send of said encrypted data and said handling policy data, sent from said data sending device; and

receiving end controlling means for verifying said received signature.

25. The information receiving device according to Claim 24, characterized in that said receiving end controlling means compares creator identification data included in said data with creator identification data included in said handling policy data.

26. The information receiving device according to Claim 24, characterized in that

said receiving means receives the signature for said encrypted data and said handling policy data, sent from said data sending device, and

said receiving end controlling means verifies the signature for said encrypted data and said handling policy data.

27. The information receiving device according to Claim 24, characterized in that

said receiving means receives the signature for said encrypted data and the signature for said handling policy data, sent from said data sending device and

said receiving end controlling means verifies the signature for said encrypted data and the signature for said handling policy data.

28. The information receiving device according to Claim 24, characterized in that

said receiving means receives the signature for secure containers for said encrypted data and said handling policy data, sent from said data sending device, and

said receiving end controlling means verifies said signature for secure containers.

29. The information receiving device according to Claim 24, characterized in that

said receiving means receives the signature for data for said encrypted data, and the signature for said handling policy data and said signature for data, sent from said data sending device, and

said receiving end controlling means verifies said signature for data and said signature for handling policy.

30. The information receiving device according to Claim 24, characterized in that

said receiving means receives the signature for handling policy for said handling policy data, and the signature for data for said encrypted data and said signature for handling policy, sent from said data sending device, and

said receiving end controlling means verifies said signature for handling policy and said signature for data.

31. The information receiving device according to Claim 24, characterized in that

said receiving means receives the signature for key data for said key data encrypted with a distribution key, sent from said data sending device, and

said receiving end controlling means verifies said signature for key data.

32. The information receiving device according to Claim 28, characterized in that

said receiving means receives the signature for secure containers for said key data encrypted with a distribution key, said encrypted data and said handling policy, sent from said data sending device, and

said receiving end controlling means verifies said signature for secure containers.

33. An information sending method for sending predetermined data to a data receiving device, characterized by comprising:

a generating step of encrypting said data with predetermined key data, generating handling policy data describing handling policy of

said data, and generating a signature for send of said encrypted data and said handling policy data; and

a sending step of sending said signature to said data receiving method together with said encrypted data and said handling policy data.

34. The information sending method according to Claim 33, characterized in that

in said generating step, said data including creator identification data is encrypted with said key data, and said handling policy including said creator identification data is generated.

35. The information sending method according to Claim 33, characterized in that

in said generating step, a signature for said encrypted data and said handling policy data is generated.

36. The information sending method according to Claim 33, characterized in that

in said generating step, signatures for said encrypted data and said handling policy data are generated separately.

37. The information sending method according to Claim 33, characterized in that

in said generating step, a signature for secure container for said encrypted data and said handling policy data is generated.

38. The information sending method according to Claim 33, characterized in that

in said generating step, a signature for data for said encrypted data is generated, and a signature for handling policy for said handling policy data and said signature for data is generated.

39. The information sending method according to Claim 33, characterized in that

in said generating step, a signature for handling policy for said handling policy data is generated, and a signature for data for said encrypted data and said signature for handling policy is generated.

40. The information sending method according to Claim 33, characterized in that

in said generating step, encrypted key data with key data for encrypting said data encrypted with a distribution key is stored, and a signature for key data for said encrypted key data is generated, and

in said sending step, said generated signature for key data is sent to said data receiving device.

41. The information sending method according to Claim 37, characterized in that

in said generating step, encrypted key data with key data for encrypting said data encrypted with a distribution key is stored, and a signature for secure containers for said encrypted data, said encrypted key data and said handling policy is generated, and

in said sending step, said encrypted data, said encrypted key data, said handling policy data, and said signature for secure containers are sent to said data receiving device.

42. An information receiving method for receiving predetermined data sent from a data sending device, characterized by comprising:

a receiving step of receiving said data encrypted with predetermined key data, handling policy data describing handling policy of said data, and a signature for send of said encrypted data and said handling policy data, sent from said data sending device; and

a verifying step of verifying said received signature.

43. The information receiving method according to Claim 42, characterized in that

in said verifying step, creator identification data included in said data is compared with creator identification data included in said handling policy data.

44. The information receiving method according to Claim 42, characterized in that

in said receiving step, the signature for said encrypted data and said handling policy data, sent from said data sending device is received, and

in said verifying step, the signature for said encrypted data and said handling policy data is verified.

45. The information receiving method according to Claim 42, characterized in that

in said receiving step, the signature for said encrypted data and the signature for said handling policy data, sent from said data sending device are received, and

in said verifying step, the signature for said encrypted data and the signature for said handling policy data are verified.

46. The information receiving method according to Claim 42, characterized in that

in said receiving step, the signature for secure containers for said encrypted data and said handling policy data, sent from said data sending device is received, and

in said verifying step, said signature for secure containers is verified.

47. The information receiving method according to Claim 42, characterized in that

in said receiving step, the signature for data for said encrypted data, and the signature for handling policy for said handling policy data and said signature for data, sent from said data sending device are received, and

in said verifying step, said signature for data and said signature for handling policy are verified.

48. The information receiving method according to Claim 42, characterized in that

in said receiving step, the signature for handling policy for said handling policy data, and the signature for data for said encrypted data and said signature for handling policy, sent from said data sending device are received, and

in said verifying step, said signature for handling policy and said signature for data are verified.

49. The information receiving method according to Claim 42, characterized in that

in said receiving step, the signature for key data for said key data encrypted with a distribution key, sent from said data sending device is received, and

in said verifying step, said signature for key data is verified.

50. The information receiving method according to Claim 46, characterized in that

in said receiving step, the signature for secure containers for said key data encrypted with a distribution key, said encrypted data and said handling policy, sent from said data sending device is received, and

in said verifying step, said signature for secure containers is verified.

51. A program storing medium for making an information sending device run a program, characterized by comprising:

a generating step of encrypting predetermined data with predetermined key data, generating handling policy data describing handling policy of said data, and generating a signature for send of said encrypted data and said handling policy data; and

a sending step of sending said signature to said data receiving method together with said encrypted data and said handling policy data.

52. The program storing medium according to Claim 51, characterized in that

in said generating step, said data including creator identification data is encrypted with said key data, and said handling policy data including said creator identification data is generated.

53. The program storing medium according to Claim 51, characterized in that

in said generating step, a signature for said encrypted data and said handling policy data is generated.

54. The program storing medium according to Claim 51, characterized in that

in said generating step, signatures for said encrypted data and said handling policy data are generated separately.

55. The program storing medium according to Claim 51, characterized in that

in said generating step, a signature for secure containers for said encrypted data and said handling policy data is generated.

56. The program storing medium according to Claim 51, characterized in that

in said generating step, a signature for data for said encrypted data is generated, and a signature for handling policy for said handling policy data and said signature for data is generated.

57. The program storing medium according to Claim 51, characterized in that

in said generating step, a signature for handling policy for said handling policy data is generated, and a signature for data for said encrypted data and said signature for handling policy is generated.

58. The program storing medium according to Claim 51, characterized in that

in said generating step, encrypted key data with key data for encrypting said data encrypted with a distribution key is stored, and a signature for said encrypted key data is generated, and

in said sending step, said generated signature for key data is sent to said data receiving device.

59. The program storing medium according to Claim 55, characterized in that

in said generating step, encrypted key data with key data for encrypting said data encrypted with a distribution key is stored, a signature for secure containers for said encrypted data, said encrypted key data and said handling policy is generated, and

in said sending step, said encrypted data, said encrypted key data, said handling policy data, and said signature for secure containers are sent to said data receiving device.

60. A program storing medium for making an information receiving device run a program, characterized by comprising:

a receiving step of receiving predetermined data encrypted with predetermined key data, handling policy data describing handling policy of the data, and the signature for send of said encrypted data and said handling policy data, sent from said data sending device, and

a verifying step of verifying said received signature.

61. The program storing medium according to Claim 60, characterized in that

in said verifying step, creator identification data included in said data is compared with creator identification data included in said handling policy data.

62. The program storing medium according to Claim 60, characterized in that

in said receiving step, the signature for said encrypted data and said handling policy data, sent from said data sending device is received, and

in said verifying step, the signature for said encrypted data and said handling policy data is verified.

63. The program storing medium according to Claim 60, characterized in that

in said receiving step, the signature for said encrypted data and the signature for said handling policy data, sent from said data sending device are received, and

in said verifying step, the signature for said encrypted data and the signature for said handling policy data are verified.

64. The program storing medium according to Claim 60, characterized in that

in said receiving step, the signature for secure containers for said encrypted data and said handling policy data, sent from said data sending device is received, and

in said verifying step, said signature for secure containers is verified.

65. The program storing medium according to Claim 60, characterized in that

in said receiving step, the signature for data for said encrypted data, and the signature for handling policy for said handling policy data and said signature for data , sent from said data sending device are received, and

in said verifying step, said signature for data and said signature for handling policy are verified.

66. The program storing medium according to Claim 60, characterized in that

in said receiving step, the signature for handling policy for said handling policy data, and the signature for data for said encrypted data and said signature for handling policy, sent from said data sending device are received, and

in said verifying step, said signature for handling policy and said signature for data are verified.

67. The program storing medium according to Claim 60, characterized in that

in said receiving step, the signature for key data for said key data encrypted with a distribution key, sent from said data sending device is received, and

in verifying step, said signature for key data is verified.

68. The program storing medium according to Claim 64, characterized in that

in said receiving step, the signature for secure containers for said key data encrypted with a distribution key, and said encrypted data and said handling policy, sent from said data sending device is received, and

in said verifying step, said signature for secure containers is verified.

69. An information distribution system for distributing predetermined data from an information sending device to an information receiving device, characterized in that

said information sending device comprises

sending means for sending send data including said data encrypted with key data for distribution given in advance, and

said information receiving device comprises:

receiving means for receiving said send data; and

receiving end controlling means for decrypting said data using said key data given in advance.

70. An information distribution method for distributing predetermined data from an information sending device to an information receiving device, characterized by comprising:

a sending step of sending send data including said data encrypted with key data for distribution given in advance, by said information sending device; and

a decrypting step of receiving said send data, and decrypting said data using said key data given in advance, by said information receiving device.

71. An information sending device for sending predetermined data to an information receiving device, characterized by comprising:

sending end controlling means for generating send data including said data encrypted using key data for distribution given in advance to said information receiving device; and

sending means for sending said send data.

72. The information sending device according to Claim 71, characterized in that

said sending end controlling means generates send data including an individual key specific to said information sending device, as said data encrypted with said key data.

73. The information sending device according to Claim 72, characterized in that

said sending end controlling means generates send data including said data encrypted using said key data that is periodically updated.

74. The information sending device according to Claim 73, characterized in that

said sending end controlling means generates said send data including said encrypted data using said key data appropriate to an update period, in said data encrypted using said key data for a plurality of update periods given in advance together.

75. An information receiving device for receiving predetermined data sent from an information sending device, characterized by comprising:

receiving means for receiving send data including said data encrypted with key data for distribution, sent from said information sending device; and

receiving end controlling means for decrypting said data using said key data given in advance.

76. The information receiving device according to Claim 75, characterized in that

said receiving means receives send data including an individual key specific to said information receiving device, as said data encrypted with said key data.

77. The information receiving device according to Claim 76, characterized in that

said receiving means receives said send data including said data encrypted with said key data that is periodically updated, and

said receiving end controlling means decrypts said data using said key data that is periodically updated and given.

78. The information receiving device according to Claim 77, characterized in that

said receiving end controlling means decrypts said data using said key data appropriate to an update period, in said key data for plurality of update periods given in advance.

79. An information sending method for sending predetermined data to an information receiving device, characterized by comprising:

a generating step of generating send data including said data encrypted using key data for distribution given in advance to said information receiving device; and

a sending step of sending said send data.

80. The information sending method according to Claim 79, characterized in that

in said generating step, send data including an individual key specific to said information sending device is generated as said data encrypted with said key data.

81. The information sending method according to Claim 80, characterized in that

in said generating step, send data including said data encrypted using said key data that is updated periodically is generated.

82. The information sending method according to Claim 81, characterized in that

in said generating step, said send data including said data encrypted using said key data appropriate to an update period, in said data encrypted using said key data for a plurality of update periods given together in advance, is generated.

83. An information receiving method for receiving predetermined data sent from an information sending device, characterized by comprising:

a receiving step of receiving send data including said data encrypted with key data for distribution, sent from said information sending device; and

a decrypting step of decrypting said data using said key data given in advance.

84. The information receiving method according to Claim 83, characterized in that

in said receiving step, send data including an individual key specific to said information receiving device is received as said data encrypted with said key data.

85. The information receiving method according to Claim 84, characterized in that

in said receiving step, said send data including said data encrypted with said key data that is updated periodically is received, and

in said decrypting step, said data is decrypted using said key data that is periodically updated and given.

86. The information receiving method according to Claim 85, characterized in that

in said decrypting step, said data is decrypted using said key data appropriate to an update period, in said key data for a plurality of update periods given together in advance.

87. A program storing medium for making an information sending device run a program, characterized by comprising:

a generating step of generating send data including predetermined data encrypted using key data for distribution given in advance to an information receiving device; and

a sending step of sending said send data to said information receiving device.

88. The program storing medium according to Claim 87, characterized in that

in said generating step, send data including an individual key specific to said information sending device is generated as said data encrypted with said key data.

89. The program storing medium according to Claim 88, characterized in that

in said generating step, send data including said data encrypted using said key data that is updated periodically is generated.

90. The program storing medium according to Claim 89, characterized in that

in said generating step, said send data including said data encrypted using said key data appropriate to an update period, in said data encrypted using said key data for a plurality of update periods given together in advance is generated.

91. A program storing medium for making an information receiving device run a program, characterized by comprising:

a receiving step of receiving send data including predetermined data encrypted with key data for distribution, sent from an information sending device; and

a decrypting step of decrypting said data using said key data given in advance.

92. The program storing medium according to Claim 91, characterized in that

in said receiving step, send data including an individual key specific to said information receiving device is received as said data encrypted with said key data.

93. The program storing medium according to Claim 92, characterized in that

in said receiving step, said send data including said data encrypted with said key data that is updated periodically is received, and

in said decrypting step, said data is decrypted using said key data that is periodically updated and given.

94. The program storing medium according to Claim 93, characterized in that

in said decrypting step, said data is decrypted using said key data appropriate to an update period, in said key data for plurality of update periods given together in advance.

95. An information distribution system for distributing predetermined content data from an information sending device to an information receiving device, characterized in that

said information sending device comprises:

sending end controlling means for encrypting said content data with a content key, and encrypting the content key with an individual key specific to said information sending device; and

sending means for sending an encrypted individual key made by encrypting said individual key with a predetermined distribution key, which is supplied from the outside, to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key, and

said information receiving device comprises:

receiving means for receiving said content data encrypted with said content key and said content key encrypted with said individual key together with said encrypted individual key; and

receiving end controlling means for decrypting said individual key with said distribution key given in advance, decrypting said content key with the decrypted individual key, and decrypting said content data with the decrypted content key.

96. An information distribution method for distributing predetermined content data from an information sending device to an information receiving device, characterized by comprising:

a sending step of encrypting said content data with a content key, encrypting the content key with an individual key specific to said information sending device, and sending an encrypted individual key made by encrypting said individual key with a predetermined distribution key, which is supplied from the outside, to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key, by said information sending device; and

a decrypting step of receiving said content data encrypted with said content key and said content key encrypted with said individual key together with said encrypted individual key, decrypting said individual key with said distribution key given in advance, decrypting said content key with the decrypted individual key, and decrypting said content data with the decrypted content key, by said information receiving device.

97. An information sending device for sending predetermined content data to an information receiving device, characterized by comprising:

sending end controlling means for encrypting said content data with a content key, and encrypting the content key with an individual key specific to said information sending device; and

sending means for sending an encrypted individual key made by encrypting said individual key with a predetermined distribution key, which is supplied from the outside, to said information receiving means together with said content data encrypted with said content key and said content key encrypted with said individual key.

98. The information sending device according to Claim 97, characterized in that

said sending end controlling means encrypts said content key with said individual key supplied from the outside together with said encrypted individual key.

99. The information sending device according to Claim 98, characterized in that

said sending means sends said encrypted individual key made by encrypting said individual key with said distribution key that is updated periodically, which is supplied from the outside, to said information receiving device together with said content data encrypted with said content key and said content key encrypted with said individual key.

100. The information sending device according to Claim 99, characterized in that

said sending means sends said encrypted individual key appropriate to an update period, in said encrypted individual key for a plurality of periods given together in advance to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

101. An information receiving device for receiving predetermined content data sent from an information sending device, characterized by comprising:

receiving means for receiving said content data encrypted with a content key, said content key encrypted with an individual key specific to said information sending device, and said individual key encrypted with a predetermined distribution key, sent from said information sending device; and

receiving end controlling means for decrypting said individual key with said distribution key given in advance, decrypting said content key with the decrypted individual key, and decrypting said content data with the decrypted content key.

102. The information receiving device according to Claim 101, characterized in that

said receiving end controlling means decrypts said individual key with said distribution key that is updated periodically.

103. The information receiving device according to Claim 102, characterized in that

said receiving end controlling means decrypts said individual key with said distribution key appropriate to an update period, in said distribution key for a plurality of periods given together in advance.

104. An information sending method for sending predetermined content data to an information receiving device, characterized by comprising:

a encrypting step of encrypting said content data with a content key, and encrypting the content key with an individual key specific to said information sending device; and

a sending step of sending an encrypted individual key made by encrypting said individual key with predetermined distribution key, which is supplied from the outside, to said information receiving device together with said content data encrypted with said content key and said content key encrypted with said individual key.

105. The information sending method according to Claim 104, characterized in that

in said encrypting step, said content key is encrypted with said individual key supplied from the outside together with said encrypted individual key.

106. The information sending method according to Claim 105, characterized in that

in said sending step, said encrypted individual key made by encrypting said individual key with said distribution key that is updated periodically, which is supplied from the outside, is sent to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

107. The information sending method according to Claim 106, characterized in that

in said sending step, said encrypted individual key appropriate to an update period, in said encrypted individual key for a plurality of update periods given together in advance, is sent to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

108. An information receiving method for receiving predetermined content data sent from an information sending device, characterized by comprising:

a receiving step of receiving said content data encrypted with a content key, said content key encrypted with an individual key specific to said information sending device, and said individual key encrypted with a predetermined distribution key, sent from said information sending device; and

a decrypting step of decrypting said individual key encrypted with said distribution key given in advance, decrypting said content key

with the decrypted individual key, and decrypting said content data with the decrypted content key.

109. The information receiving method according to Claim 108, characterized in that

in said decrypting step, said individual key is decrypted with said distribution key that is updated periodically.

110. The information receiving method according to Claim 109, characterized in that

in said decrypting step, said individual key is decrypted with said distribution key appropriate to an update period, in said distribution key for a plurality of update periods given together in advance.

111. A program storing medium for making an information sending device run a program; characterized by comprising:

an encrypting step of encrypting predetermined content data with a content key, and encrypting the content key with an individual key specific to an information sending device; and

a sending step of sending an encrypted individual key made by encrypting said individual key with a predetermined distribution key, which is supplied from the outside, to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

112. The program storing medium according to Claim 111, characterized in that

in said encrypting step, said content key is encrypted with said individual key supplied from the outside together with said encrypted individual key.

113. The program storing medium according to Claim 112, characterized in that

in said sending step, said encrypted individual key made by encrypting said individual key with said distribution key that is updated periodically, which is supplied from the outside, is sent to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

114. The program storing medium according to Claim 113, characterized in that

in said sending step, said encrypted individual key appropriate to an update period, in said encrypted individual key for a plurality of update periods given together in advance, is sent to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

115. A program storing medium for making an information receiving device run a program, characterized by comprising:

a receiving step of receiving predetermined content data encrypted with a content key, said content key encrypted with an individual key specific to said information sending device, and said individual key encrypted with a predetermined distribution key, sent from an information sending device; and

a decrypting step of decrypting said individual key with said distribution key given in advance, decrypting said content key with the decrypted individual key, and decrypting said content data with the decrypted content key.

116. The program storing medium according to Claim 115, characterized in that

in said decrypting step, said individual key is decrypted with said distribution key that is updated periodically.

117. The program storing medium according to Claim 116, characterized in that

in said decrypting step, said individual key is decrypted with said distribution key appropriate to an update period, in said distribution key for a plurality of update periods given together in advance.

118. An information distribution system for distributing content data encrypted with a predetermined content key from an information sending device to an information receiving device: characterized in that

said information receiving device comprises:

receiving end controlling means having usage right of said content data, and said content key for decrypting said content data distributed from said information sending device, and generating a playback command for another apparatuses that does not have the usage right of said content data; and

sending means for sending said playback command and said content key to said another apparatus, thereby having said content played back by said another apparatus.

119. The information distribution system according to Claim 118, characterized in that

said sending means sends said content data to said another apparatus, and

said another apparatus receives said content data encrypted with said content key from said information receiving device, and plays back the received content data using said content key and said playback command.

120. The information distribution system according to Claim 119, characterized in that

said receiving end controlling means performs, with said another apparatus, cross-examination of registration information indicating that registration is possible or not possible at the time of using said content data, and

said sending means sends said content key and said playback command to said another apparatus, if the result of examination of said registration information by said receiving end controlling means shows that use is possible, mutually.

121. An information distribution method for distributing content data encrypted with a predetermined content key from an information sending device to an information receiving device, characterized by comprising:

a generating step of generating a playback command for another apparatus that does not have usage right of said content data, by said information receiving device having usage right of said content data, and said content key for decrypting said content data distributed from said information sending device; and

a sending step of sending said playback command and said content key to said another apparatus.

122. The information distribution method according to Claim 121, characterized in that

in said sending step, said content data is sent to said another apparatus, and

a playing step of receiving said content data encrypted with said content key from said information receiving device and playing back the received content data using said content key and said playback command, by said another apparatus, is comprised.

123. The information distribution method according to Claim 122, characterized in that

in said generating step, cross examination of registration information indicating that registration is possible or not possible at the time of using said content data is performed with said another apparatus, and

in said sending step, said content key and said playback command are sent to said another apparatus, if the result of examination of said registration information shows that use is possible, mutually.

124. An information receiving device for receiving content data encrypted with a predetermined content key from an information sending device, characterized by comprising:

receiving end controlling means having said content key for decrypting said content data distributed from said information sending device, and generating a playback command for another apparatus that does not have usage right of said content data, if having usage right of said content data, and

sending means for sending said playback command and said content key to said another apparatus.

125. The information receiving device according to Claim 124, characterized in that

said receiving end controlling means examines registration information indicating that registration is possible or not possible at the time of using said content data of said another apparatus, and

said sending means sends said content key and said playback command to said another apparatus if the result of examination of said registration information by said receiving end controlling means shows that use is possible.

126. The information receiving device according to Claim 125, characterized in that

said receiving end controlling means generates said playback command including identification information of said content data that is played back by said another apparatus.

127. The information receiving device according to Claim 126, characterized in that

said receiving end controlling means encrypts said playback command and said content key with a temporary key shared with said another apparatus, and

said sending means sends said playback command and said content key encrypted with said temporary key to said another apparatus.

128. An apparatus capable of communicating with an information receiving device receiving content data encrypted with a predetermined content key from an information sending device, characterized by comprising:

receiving means for receiving a playback command and said content key sent from said information receiving device having usage right of said content data and said content key for decrypting said content data distributed from said information sending device, and receiving said content data sent from said information receiving device, if not having usage right of said content data; and

apparatus side controlling means for playing back said content data using said playback command and said content key.

129. The apparatus according to Claim 128, characterized in that

said apparatus side controlling means examines registration information indicating that registration is possible or not possible at the time of using said content data of said information receiving device, and

said receiving means receives said content key and said playback command if the result of examination of said registration information by said apparatus side controlling means shows that use is possible.

130. The apparatus according to Claim 129, characterized in that said receiving means receives said playback command including identification information of said content data to be played back, which is sent from said information receiving device.

131. The apparatus according to Claim 130, characterized in that said receiving means receives said playback command and said content key encrypted with a temporary key shared with said information receiving device, and

said apparatus side controlling means decrypts with said temporary key said playback command and said content key encrypted with said temporary key and uses the same.

132. A sending method for sending predetermined information to another apparatus from an information receiving device receiving content data encrypted with a predetermined content key from an information sending device, said sending method of an information receiving device, characterized by comprising:

a generating step of generating a playback command for another apparatus that does not have usage right of said content data, if having usage right of said content data, and said content key for decrypting said content data distributed from said information sending device; and

a sending step of sending said playback command and said content key to said another apparatus.

133. The sending method of an information receiving device according to Claim 132, characterized in that

in said generating step, registration information indicating that registration is possible or not possible at the time of using said content data of said another apparatus is examined, and

in said sending step, said content key and said playback command are sent for said another apparatus if the result of examination of said registration information by said receiving end controlling means shows that use is possible.

134. The sending method of an information receiving device according to Claim 133, characterized in that

in said generating step, said playback command including identification information of said content data that is played back by said another apparatus is generated.

135. The sending method of an information receiving device according to Claim 134, characterized in that

in said generating step, said playback command and said content key are encrypted with a temporary key shared with said another apparatus, and

in said sending step, said playback command and said content key encrypted with said temporary key are sent to said another apparatus.

136. A playback method of an apparatus capable of communicating with an information receiving device receiving content data encrypted

with a predetermined content key from an information sending device, characterized by comprising:

a receiving step of receiving a playback command and said content key sent from said information receiving device having usage right of said content data, and said content key for decrypting said content data distributed from said information sending device, and receiving said content data sent from said information receiving device, if not having usage right of said content data; and

a playing step of playing back said content data using said playback command and said content key.

137. The playback method of an apparatus according to Claim 136, characterized in that

in said receiving step, registration information indicating that registration is possible or not possible at the time of using said content data of said information receiving device is examined, and said content key and said playback command sent from said information receiving device are received if the result of examination of the registration information shows that use is possible.

138. The playback method of an apparatus according to Claim 139, characterized in that

in said receiving step, said playback command including identification information of said content data to be played back, which is sent from said information receiving device is received.

139. The playback method of an apparatus according to Claim 138, characterized in that

in said receiving step, said playback command and said content key encrypted with a temporary key shared with said information receiving device are received, and

in said playing step, said playback command and said content key encrypted with said temporary key are decrypted with said temporary key and are used.

140. A program storing medium for making an information receiving device run a program, characterized by comprising:

a generating step if having usage right of a predetermined content data, and a predetermined content key for decrypting said content data that is encrypted with said content key and is distributed from an information sending device, generating a playback command for another apparatus that does not have usage right of said content data; and

a sending step of sending said playback command and said content key to said another apparatus.

141. The program storing medium according to Claim 140, characterized in that

in said generating step, registration information indicating that registration is possible or not possible at the time of using said content data of said another apparatus is examined, and

in said sending step, said content key and said playback command are sent to said another apparatus, if the result of examination of said registration information by said receiving end controlling means shows that use is possible.

142. The program storing medium according to Claim 141, characterized in that

in said generating step, said playback command including identification information of said content data to be played back by said another apparatus is generated.

143. The program storing medium according to Claim 142, characterized in that

in said generating step, said playback command and said content key are encrypted with a temporary key shared with said another apparatus, and

in said sending step, said playback command and said content key encrypted with said temporary key are sent to said another apparatus.

144. In a playback method of an apparatus capable of communicating with an information receiving device receiving content data encrypted with a predetermined content key from an information sending device, a program storing medium for making an apparatus capable of communicating with an information receiving device run a program, characterized by comprising:

a receiving step of receiving a playback command and said content key sent from said information receiving device having usage right of said content data, and said content key for decrypting said content data distributed from said information sending device, and receiving said content data sent from said information receiving device if not having usage right of said content data; and

a playing step of playing back said content data using said playback command and said content key,

145. The program storing medium according to Claim 144, characterized in that

in said receiving step, registration information indicating that registration is possible or not possible at the time of using said content data of said information receiving device is examined, and said content key and said playback command sent from said information receiving device are received if the result of examination of the registration information shows that use is possible.

146. The program storing medium according to Claim 145, characterized in that

in said receiving step, said playback command including identification information of said content data to be played back, which is sent from said information receiving device is received.

147. The program storing medium according to Claim 146, characterized in that

in said receiving step, said playback command and said content key encrypted with a temporary key shared with said information receiving device are received, and

in said playing step, said playback command and said content key encrypted with said temporary key are decrypted with said temporary key and are used.

148. An information distribution system for sending content data encrypted with a predetermined content key from an information sending device to an information receiving device, characterized in that

said information sending device comprises:

sending end controlling means for encrypting said content key with an individual key specific to said information sending device; and

sending means for sending at least said content key encrypted with said individual key, and an encrypted individual key made by encrypting said individual key with an distribution key that is updated in a predetermined cycle, which is supplied from the outside, to said information receiving device, and

said information receiving device comprises:

receiving means for receiving at least said content key encrypted with said individual key and said encrypted individual key; and

receiving end controlling means for decrypting said individual key with said distribution key given in advance, decrypting said content key with the decrypted individual key, and storing the decrypted content key, before said distribution key is updated, thereby making it possible to decrypt said content after said distribution key is updated.

149. An information distribution method for sending content data encrypted with a predetermined content key from an information sending device to an information receiving device, characterized by comprising:

a sending step of encrypting said content key with an individual key specific to the information sending device, and sending at least said content key encrypted with said individual key, and an encrypted

individual key made by encrypting said individual key with an distribution key that is updated in a predetermined cycle, which is supplied from the outside, to said information receiving device, by said information sending device; and

a storing step of receiving at least said content key encrypted with said individual key, and said encrypted individual key, and decrypting said individual key with said distribution key given in advance, decrypting said content key with the decrypted individual key, and storing the decrypted content key before said distribution key is updated, thereby making it possible to decrypt said content after said distribution key is updated, by said information receiving device.

150. An information receiving device for receiving content data encrypted with a content key distributed from an information sending device, characterized by comprising:

receiving means for receiving at least said content key encrypted with an individual key, and an encrypted individual key made by encrypting said individual key with a distribution key that is updated in a predetermined cycle, which are sent from said information sending device, before said distribution key is updated; and

controlling means for decrypting said individual key with said distribution key given in advance, decrypting said content key with the decrypted individual key, and storing the decrypted content key before said distribution key is updated, thereby making it possible to decrypt said content after said distribution key is updated.

151. The information receiving device according to Claim 150, characterized in that

said receiving means receives said content key encrypted with said individual key specific to said information sending device, and said encrypted individual key, before said distribution key is updated.

152. The information receiving device according to Claim 151, characterized in that

said controlling means encrypts said content key decrypted using said distribution key before said update, with a save key, and stores the same.

153. The information receiving device according to Claim 152, characterized in that

said controlling means encrypts said content key decrypted using said distribution key before said update, with said save key specific to said information receiving device, and stores the same.

154. The information receiving device according to Claim 153, characterized in that

said receiving means receives said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, together with a signature for send, and

said controlling means verifies said signature and decrypts said individual key with said distribution key given in advance, decrypts said content key with the decrypted individual key, and stores the decrypted content key, before said distribution key is updated, if it

is confirmed that said content key encrypted with said individual key, and said encrypted individual key are not tampered.

155. The information receiving device according to Claim 154, characterized in that

said receiving means receives said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, together with signatures added separately to said content key encrypted with said individual key and said encrypted individual key.

156. The information receiving device according to Claim 155, characterized in that

said receiving means receives said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, together with a signature added to both of said content key encrypted with said individual key and said encrypted individual key.

157. An information receiving method for receiving content data encrypted with a content key distributed from an information sending device, characterized by comprising:

a receiving step of receiving at least said content key encrypted with an individual key, and an encrypted individual key made by encrypting said individual key with a distribution key that is updated in a predetermined cycle, sent from said information sending device, before said distribution key is updated; and

a storing step of decrypting said individual key with said distribution key given in advance, decrypting said content key with the decrypted individual key, and storing the decrypted content key before said distribution key is updated, thereby making it possible to decrypt said content after said distribution key is updated.

158. The information receiving method according to Claim 157, characterized in that

in said receiving step, said content key encrypted with said individual key specific to said information sending device, and said encrypted individual key are received before said distribution key is updated.

159. The information receiving method according to Claim 158, characterized in that

in said storing step, said content key decrypted using said distribution key before said update is encrypted with a save key and is stored.

160. The information sending method according to Claim 159, characterized in that

in said storing step, said content key decrypted using said distribution key before said update is encrypted with said save key specific to an information receiving device and is stored.

161. The information receiving method according to Claim 160, characterized in that

in said receiving step, said content key encrypted with said individual key and said encrypted individual key, sent from said

information sending device, are received together with a signature for send, and

in said storing step, said signature is verified, and said individual key is decrypted with said distribution key given in advance, said content key is decrypted with the decrypted individual key, and the decrypted content key is stored, before said distribution key is updated, if it is confirmed that said content key encrypted with said individual key and said encrypted individual key are not tampered.

162. The information receiving method according to Claim 161, characterized in that

in said receiving step, said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device are received together with signatures added separately to said content key encrypted with said individual key and said encrypted individual key.

163. The information receiving method according to Claim 162, characterized in that

in said receiving step, said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, are received together with a signature added to both of said content key encrypted with said individual key and said encrypted individual key.

164. A program storing medium for making an information receiving device run a program, characterized by comprising:

a receiving step of receiving at least a content key encrypted with an individual key, and an encrypted individual key made by encrypting said individual key with a distribution key that is updated in a predetermined cycle, sent from an information sending device sending content data encrypted with said content key, before said distribution key is updated; and

a storing step of decrypting said individual key with said distribution key given in advance, decrypting said content key with the decrypted individual key, and storing the decrypted content key before said distribution key is updated, thereby making it possible to decrypt said content after said distribution key is updated.

165. The program storing medium according to Claim 164, characterized in that

in said receiving step, said content key encrypted with said individual key specific to said information sending device, and said encrypted individual key are received before said distribution key is updated.

166. The program storing medium according to Claim 165, characterized in that

in said storing step, said content key decrypted using said distribution key before said update is encrypted with a save key and is stored.

167. The program storing medium according to Claim 166, characterized in that

in said storing step, said content key decrypted using said distribution key before said update is encrypted with said save key specific to an information receiving device and is stored.

168. The program storing medium according to Claim 167, characterized in that

in said receiving step, said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, are received together with a signature for send, and

in said storing step, said signature is verified, and said individual key is decrypted with said distribution key given in advance, said content key is decrypted with the decrypted individual key, and the decrypted content key is stored before said distribution key is updated, if it is confirmed that said content key encrypted with said individual key and said encrypted individual key are not tampered.

169. The program storing medium according to Claim 168, characterized in that

in said receiving step, said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, are received together with signatures added separately to said content key encrypted with said individual key and said encrypted individual key.

170. The program storing medium according to Claim 169, characterized in that

in said receiving step, said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, are received together with a signature added to both of said content key encrypted with said individual key and said encrypted individual key.

171. An information receiving system for receiving content data distributed from an information sending device by first and second information receiving devices, characterized in that

said first information receiving device having usage right of said content data comprises:

first sending means for sending first registration information of said first information receiving device to said second information receiving device different in registration information for using said content data;

first receiving means for receiving second registration information of said second information receiving device; and

first controlling means for determining by said second registration information whether or not said content data for said second information receiving device can be used,

said second information receiving device comprises:

second sending means for sending said second registration information to said first information receiving device;

second receiving means for receiving said first registration information of said first information receiving device; and

second controlling means for determining by said second registration information whether or not said content data for said first information receiving device can be used, and

said first and second information receiving devices mutually determine by said first and second controlling means whether or not said content data can be used, and said usage right is sent and passed from said first sending means of said first information receiving device to said second information receiving device if said first and second information receiving devices both determine that said content data can be used, thereby making it possible to use said content data by said second information receiving device.

172. The information receiving system according to Claim 171, characterized in that

said first controlling means of said first information receiving device generates and retains accounting information for used part of said content data that is used by said second information receiving device for which it is determined that said content data can be used.

173. The information receiving system according to Claim 171, characterized in that

said second controlling means of said second information receiving device generates and retains accounting information for used part of said content data.

174. A content using method, characterized by comprising:

a determining step of exchanging registration information among a plurality of said information receiving devices different from each

other in said registration information for using content data distributed from an information sending device, thereby mutually determining whether or not said content data can be used among a plurality of said information receiving devices; and

a passing step of passing usage right to a second information receiving device for which a first information receiving device having said usage right of said content data in a plurality of said information receiving devices determines that said content data can be used, thereby making it possible to use said content data by said second information receiving device to which said usage right is passed.

175. The content using method according to Claim 174, characterized in that

said first information receiving device having usage right of said content data comprises a retaining step of generating and retaining accounting information for used part of said content data that is used by said second information receiving device for which it is determined that said content data can be used.

176. The content using method according to Claim 174, characterized in that

said second information receiving device that receives usage right of said content data comprises a retaining step of generating and retaining accounting information for used part of said content data.

177. An information receiving device for receiving content data distributed from an information sending device, characterized by comprising:

sending means for sending its first registration information to other information receiving devices different in registration information for using said content data;

receiving means for receiving second registration information of said other information receiving devices; and

controlling means for determining by said first and second registration information whether or not said content data can be used, mutually with said other information receiving devices,

in which if having usage right of said content data, said controlling means passes said usage right through said sending means to said other information receiving devices for which it is determined that said content data can be used, thereby making it possible to use said content data by said other information receiving devices to which said usage right is passed.

178. The information receiving device according to Claim 177, characterized in that

said controlling means generates and retains accounting information for used part of said content data that is used by said other information receiving devices to which usage right of said content data is passed.

179. The information receiving device according to Claim 178, characterized in that

said controlling means retains said content data encrypted with a predetermined content key, handling policy data describing handling policy of said content key, and price information of said content data,

and generates and retains said accounting information based on said handling policy data and said price information.

180. The information receiving device according to Claim 179, characterized in that

said controlling means generates license condition information describing usage right of said content data based on said handling policy data and said price information, and

said sending means sends said license condition information to said other information receiving devices as usage right of said content data.

181. The information receiving device according to Claim 180, characterized in that

said controlling means encrypts said content key with a temporary key shared with said other information receiving devices, and

said sending means sends said content data encrypted with said content key and said content key encrypted with said temporary key to said other information receiving devices together with said license condition information.

182. The information receiving device according to Claim 177, characterized in that

said controlling means retains said content data encrypted with a predetermined content key, handling policy data describing handling policy of said content key, and price information of said content data, and

said sending means sends said handling policy data and said price information for generating license condition information describing usage right of said content data and accounting information for used part of said content data to said other information receiving devices.

183. The information receiving device according to Claim 182, characterized in that

said controlling means encrypts said content key with a temporary key shared with said other information receiving devices, and

said sending means sends said content data encrypted with said content key and said content key encrypted with said temporary key to said other information receiving devices together with said handling policy data and said price information.

184. An information receiving device for receiving content data distributed from an information sending device, characterized by comprising:

sending means for sending its first registration information to other information receiving devices different in registration information for using said content data;

receiving means for receiving second registration information of said other information receiving devices; and

controlling means for determining by said first and second registration information whether or not said content data con be used, mutually with said other information receiving devices,

in which if not having usage right of said content data , said usage right sent from an information receiving device having usage right

of said content data, in said other information receiving devices for which it is determined that said content data can be used, is received by said receiving means to make it possible to use said content data.

185. The information receiving device according to Claim 184, characterized in that

said controlling means generates and retains accounting information for used part of said content data.

186. The information receiving device according to Claim 185, characterized in that

said receiving means receives handling policy data describing handling policy of a predetermined content key encrypting said content data, and price information of said content data, sent from an information receiving device having usage right of said content data, and

said controlling means generates and retains said accounting information based on said handling policy data and said price information.

187. The information receiving device according to Claim 186, characterized in that

said controlling means generates and retains license condition information describing usage right of said content data based on said handling policy data and said price information.

188. The information receiving device according to Claim 187, characterized in that

said receiving means receives said content data encrypted with said content key, and said content key encrypted with a temporary key shared with said other information receiving devices, sent from an information receiving device having usage right of said content data, and

said sending means decrypts said content key with said temporary key, encrypts the said decrypted content key with its specific save key and stores the same, and retains said content data encrypted with said content key.

189. A content using method of an information receiving device for receiving content data distributed from an information sending device, characterized by comprising:

an exchanging step of exchanging said registration information with other information receiving devices different in registration information for using said content data;

a determining step of determining by said registration information whether or not said content data can be used, mutually with other information receiving devices; and

a passing step of passing usage right to said other information receiving devices for which it is determined that said content data can be used, thereby making it possible to use said content data by said other information receiving devices to which said usage right is passed, if having said usage right of said content data.

190. The content using method according to Claim 189, characterized by comprising:

a generating and retaining step of generating and retaining accounting information for used part of said content data that is used by said other information receiving devices to which usage right of said content data is passed.

191. The content using method according to Claim 190, characterized in that

in said generating and retaining step, said accounting information is generated based on handling policy data describing handling policy of said content key retained together with said content data encrypted with the predetermined content key, and price information of said content data, and is retained.

192. The content using method according to Claim 191, characterized in that

a generating step of generating license condition information describing usage right of said content data based on said handling policy data and said price information is comprised, and

in said passing step, said license condition information is passed to said other information receiving devices as usage right of said content data.

193. The content using method according to Claim 192, characterized in that

an encrypting step of encrypting said content key with a temporary key shared with said other information receiving devices is comprised, and

in said passing step, said content data encrypted with said content key, and said content key encrypted with said temporary key is sent to said other information receiving devices together with said license condition information.

194. The content using method according to Claim 189, characterized in that

in said passing step, handling policy data describing handling policy of the content key retained together with said content data encrypted with the predetermined content key, and price information of said content data are passed to said other information receiving devices in order that license condition information describing usage right of said content data, and accounting information for used part of said content data are generated.

195. The content using method according to Claim 194, characterized in that

an encrypting step of encrypting said content key with a temporary key shared with said other information receiving devices is comprised, and

in said passing step, said content data encrypted with said content key, and said content key encrypted with said temporary key are passed to said other information receiving devices, together with said handling policy data and said price information.

196. A content using method of an information receiving device for receiving content data distributed from an information sending device, characterized by comprising:

an exchanging step of exchanging said registration information with other information receiving devices different in registration information for using said content data;

a determining step of determining by said registration information whether or not said content data can be used, mutually with said other information receiving devices; and

a receiving step of receiving said usage right of said content data from an information receiving device having said usage right of said content data, in said other information receiving devices for which it is determined that said content data can be used, and making it possible to use said content data, if not having said usage right of said content data.

197. The content using method according to Claim 196, characterized by comprising:

a generating and retaining step of generating and retaining accounting information for used part of said content data.

198. The content using method according to Claim 197, characterized in that

in said receiving step, handling policy data describing handling policy of a predetermined content key encrypting said content data, and price information of said content data, sent from an information receiving device having usage right of said content data are received, and

in said generating and retaining step, said accounting information is generated based on said handling policy data and said price information and is retained.

199. The content using method according to Claim 198, characterized by comprising:

an information generating step of generating and retaining license condition information describing usage right of said content data, based on said handling policy data and said price information.

200. The content using method according to Claim 197, characterized in that

in said receiving step, said content data encrypted with said content key, and said content key encrypted with a temporary key shared with said other information receiving devices, sent from an information receiving device having usage right of said content data, are received, and

a content retaining step of decrypting said content key with said temporary key, encrypting the decrypted content key with its specific save key and storing the same, and retaining said content data encrypted with said content key is comprised.

201. A program storing medium used in an information receiving device for receiving content data distributed from an information sending device, said program storing medium making an information receiving device run a program, characterized by comprising:

an exchanging step of exchanging said registration information with other information receiving devices different in registration information for using said content data;

a determining step of determining by said registration information whether or not said content data can be used, mutually with said other information receiving devices; and

a passing step of passing usage right of said content to said other information receiving devices for which it is determined that said content data can be used, thereby making it possible to use said content data by said other information receiving devices to which said usage right is passed, if having said usage right of said content data.

202. The program storing medium according to Claim 201, characterized by comprising:

a generating and retaining step of generating and retaining accounting information for used part of said content data that is used by said other information receiving devices to which usage right of said content data is passed.

203. The program storing medium according to Claim 202, characterized in that

in said generating and retaining step, said accounting information is generated based on handling policy data describing handling policy of the content key retained together with said content data encrypted with the predetermined content key, and price information of said content data, and is retained.

204. The program storing medium according to Claim 203, characterized in that

a generating step of generating license condition information describing usage right of said content data based on said handling policy and said price information is comprised, and

in said passing step, said license condition information is passed to said other information receiving devices as usage right of said content data.

205. The program storing medium according to Claim 204, characterized in that

an encrypting step of encrypting said content key with a temporary key shared with said other information receiving devices is comprised, and

in said passing step, said content data encrypted with said content key, and said content key encrypted with said temporary key are sent to said other information receiving devices together with said license condition information.

206. The program storing medium according to Claim 201, characterized in that

in said passing step, handling policy data describing handling policy of the content key retained together with said content data encrypted with the predetermined content key, and price information of said content data are passed to said other information receiving devices in order that license condition information describing usage

right of said content data, and accounting information for used part of said content data are generated.

207. The program storing medium according to Claim 206, characterized in that

an encrypting step of encrypting said content key with a temporary key shared with said other information receiving devices is comprised, and

in said passing step, said content data encrypted with said content key, and said content key encrypted with said temporary key are passed to said other information receiving devices together with said handling policy data and said price information.

208. A program storing medium used in an information receiving device receiving content data distributed from an information sending device, said program storing medium making the information receiving device run a program, characterized by comprising:

an exchanging step of exchanging said registration information with other information receiving devices different in registration information for using said content data;

a determining step of determining by said registration information whether or not said content data can be used, mutually with said other information receiving devices; and

a receiving step of receiving said usage right of said content data from an information receiving device having said usage right of said content data, in said other information receiving devices for which it is determined that said content data can be used, and making it

possible to use said content data, if not having said usage right of said content data.

209. The program storing medium according to Claim 208, characterized by comprising:

a generating and retaining step of generating and retaining accounting information for used part of said content data.

210. The program storing method according to Claim 209, characterized in that

in said receiving step, handling policy data describing handling policy of a predetermined content key encrypting said content data, and price information of said content data, sent from an information receiving device having usage right of said content data, are received, and

in said generating and retaining step, said accounting information is generated based on said handling policy data and said price information, and is retained.

211. The program storing medium according to Claim 210, characterized by comprising:

an information generating step of generating license condition information describing usage right of said content data based on said handling policy data and said price information, and retaining the same.

212. The program storing medium according to Claim 211, characterized in that

in said receiving step, said content data encrypted with said content key, and said content key encrypted with a temporary key shared

with said other information receiving devices, sent from an information receiving device having usage right of said content data, are received, and

a content retaining step of decrypting said content key with said temporary key, encrypting the decrypted content key with its specific save key and storing the same, and retaining said content data encrypted with said content key is comprised.

213. The information sending system according to Claim 2, characterized in that

said sending end controlling means stores encrypted key data with key data for encrypting said data encrypted with a distribution key, and generates a signature for key data for said encrypted key data,

said sending means sends said generated signature for key data to said data receiving device,

said receiving means receives said key data, and

said receiving end controlling means verifies said signature for key data.

214. The information sending system according to claim 4, characterized in that

said sending end controlling means stores encrypted key data with key data for encrypting said data encrypted with a distribution key, and generates a signature for key data for said encrypted key data,

said sending means sends said generated signature for key data to said data receiving device,

said receiving means receives said key data, and

said receiving end controlling means verifies said signature for key data.

215. The information sending system according to claim 5, characterized in that

said sending end controlling means stores encrypted key data with key data for encrypting said data encrypted with a distribution key, and generates a signature for key data for said encrypted key data,

said sending means sends said generated signature for key data to said data receiving device,

said receiving means receives said key data, and

said receiving end controlling means verifies said signature for key data.

216. The information sending method according to claim 9, characterized in that

in said sending step, encrypted key data with key data for encrypting said data with a distribution key is stored, a signature for key data for said encrypted key data is generated, and the generated signature for key data is sent to said data receiving device, and

in said verifying step, said signature for key data is verified.

217. The information sending method according to claim 11, characterized in that

in said sending step, encrypted key data with key data for encrypting said data with a distribution key is stored, a signature for key data for said encrypted key data is generated, and the generated signature for key data is sent to said data receiving device, and

in said verifying step, said signature for key data is verified.

218. The information sending method according to claim 12, characterized in that

in said sending step, encrypted key data with key data for encrypting said data with a distribution key is stored, a signature for key data for said encrypted key data is generated, and the generated signature for key data is sent to said data receiving device, and

in said verifying step, said signature for key data is verified.